

6/8/02 [Changes made from must C to E cannot be followed ?
8/2/02

1. (Third time Amended) A method for protecting software from unauthorised use, *changes*

comprising the steps of:

[the electronic of]

determining if identity means/information, is existing in a processing device;

[under control of said computer]

using a favourable result of said determination as a pre-condition for said

processing device providing user access to said software desired to be protected;

wherein said identity means/information being [essentially] used by a control means of said processing device for

enabling operation(s) for which rightful user(s) of said software desired to be protected has to be responsible;

wherein access to said software desired to be protected is being provided without causing a said operation being performed and said identity means/information being specific to said rightful user(s).

7. (Third time Amended) Protection software for use on a processing device, to protect software publicly distributed by a system against unauthorised use;

said protection software comprising:

identity software [essentially] used on said processing device in enabling operation(s) for which rightful user(s) of said software desired to be protected has to be responsible;

authorising software effectively under the control of the user thereof for, when executed, providing user access to said software desired to be protected;

wherein said identity software and said authorising software are contained in said protection software in such a manner that said authorising software is prevented from being copied therefrom individually; and

wherein the improvement resides in said protection depends on no hardware specific to said user(s) and said identity software being specific to said rightful user(s).

10. (Third time Amended) Authorising program/means used in a processing device, to protect other software against unauthorised use ;

said authorising program/means being [effectively under the control of the user thereof] for providing access to said software desired to be protected ;

wherein information [related] specific to rightful user(s) of said software desired to be protected, exists in said authorising program/means and being accessible to the user thereof ;

said information being capable of being used [essentially], but not in a form to be so used , by said processing device in enabling operation(s) for which said rightful user(s) has to be responsible .

12. (Second time Amended) A method for protecting software from unauthorised use , comprising the steps of :

obtaining a first information from a user of a processing device having an identity software/means ;

using said first information received being correct as a pre-condition for said processing device providing user access to said software desired to be protected;

wherein said identity software/means being for providing a second information [related] specific to rightful user(s) of said software desired to be protected, if said correct first information is being obtained from a user thereof ;

and said second information being [essentially] used by said processing device in enabling operation(s) for which said rightful user(s) has to be responsible ;

wherein access to said software desired to be protected is being provided without causing a said operation being performed.

OFFICIAL

14. (Second time Amended) A method for protecting software from unauthorised use , comprising the steps of :

authenticating identity information/means associated with a control means of a processing device ;

using a favourable result of said authentication as a pre-condition for said control means providing user access to said software desired to be protected ;

wherein said identity information/means being [essentially] used by said control means for enabling operation(s) for which rightful user(s) of said software desired to be protected has to be responsible ;

wherein access to said software desired to be protected is being provided without causing a said operation being performed and said identity information/means being specific to said rightful user(s) .

16. (Third time Amended) A method for protecting software distributed by a system from unauthorised use , comprising the steps of :

[a] obtaining by a processing means of said system, confidential information of rightful user(s) of said software desired to be protected ;]

[b)]

a) creating [by said processing means,] first software with said confidential information of rightful user(s) of said software desired to be protected therein ;

[c)] [transferring from said system,]

b) running said first software [to] on a processing device ;

[d) thereafter,]

c) obtaining by said first software running on said processing device , first information from the user thereof ;

[e)]

d) determining by said first software, from said processing device second information related to the hardware or/and software thereof for future reference in

step f) below, in response to said first information obtained being consistent with said confidential information therein ;

[f]]

g) thereafter, authenticating by second software, the processing device on which said second software is being used, basing on at least a part of said second information ;

[h]]

f) using, by said second software, a favourable result of said authentication as a pre-condition for permitting use of said software desired to be protected on the processing device on which said second software is being used ;

wherein said confidential information is necessary for enabling electronic transaction(s) for which said rightful user(s) has to be responsible ; and said steps (d) to h)) c) to f) is being performed without causing a said [transaction] transaction take place .

20. (Second time Amended) A method for protecting software distributed by a system from unauthorised use, comprising the steps of :

a) creating by said system, first software ;

wherein "the presence of identity information/means which being [essentially] specific to a rightful user of said software desired to be protected and being used [by a control means of a processing device] for enabling operation(s) for which [a] said rightful user [of said software desired to be protected] has to be responsible, in [said] a processing device" ; is being used in the creation of said first software as a pre-condition for said first software to perform step c) below ;

b) transferring from said system, said first software to said processing device ;

c) determining by said first software running on said processing device meeting said precondition, first information related to the hardware or/and software of said processing device , for future reference in step e) below ;

- d) thereafter, determining by second software, from the processing device onwhich said second software is being used, second information related to the hardware or/and software thereof;
 - e) determining by said second software, if said second information is consistent with said first information ;
 - f) using by said second software, a favourable result of said determination of consistence as a pre-condition for permitting use of said software desired to be protected on the processing device onwhich said second software is being used ;
- repeat at least said steps c) to f) if said result of said determination of consistence is not favourable, without causing any operation(s) for which said rightful user has to be responsible, being performed ;
- wherein said first and second software being specific to said rightful user.